

ABSTRACT

A method and apparatus for data security for a distributed file system. A distributed file system interface is coupled to the one or more client applications, and a storage server and a meta-data server are coupled to the distributed file system interface. The meta-data server receives open-file requests from the distributed file system interface and in response creates a security object. The meta-data server also generates an partial encryption key and stores the partial encryption key in the security object. The block storage server completes the encryption key, and the meta-data server encrypts the list of blocks that are in the file and stores the encrypted block list in the security object. The security object is then returned to the distributed file interface and used in subsequent file access requests.